Background Note

Agenda Item: 3

To: Cyber Insurance PG

From: General Insurance Team
Meeting: 1 December 2017
Reference: GEN-CYB-17-045

Subject: Insurance Europe views on the EC Cybersecurity Act

Objective

For information and discussion

Input requested

Members will be invited to share their views on the EC Cybersecurity Act and suggest topics where Insurance Europe could develop a position.

Summary

The EC published in September its Joint Communication to the European Parliament and the Council on Resilience, deterrence and defence: building strong cybersecurity for the EU, which updates the 2013 EU Cybersecurity Strategy. At the same time, it published a proposal for a Regulation on ENISA, the new "EU Cybersecurity Agency", which reviews ENISA's mandate and expands it to ICT cybersecurity certification; the EU "Cybersecurity Act".

Joint Communication on Cybersecurity

The document lists the following key actions:

- Full implementation of the Directive on the Security of Network and Information Systems (NIS);
- A joint Commission/industry initiative to define a "duty of care" principle for reducing product/software vulnerabilities and promoting "security by design";
- Swift implementation of the blueprint for cross-border major incident response
- Launch an impact assessment to study the possibility for a Commission proposal in 2018 to set up a Network of Cybersecurity competence centres and a European Cybersecurity Research and Competence Centre
- An EU-wide one-stop-shop to help victims of cyber-attacks, providing information on latest threats and bringing together practical advice and cybersecurity tools
- Action by Member States to mainstream cybersecurity into skills programmes, e-government and awareness campaigns
- A Commission initiative for cross-border access to electronic evidence (early 2018)
- A cybersecurity-related education platform to address the current skills gap in cybersecurity and cyber defence in 2018
- Enhance international cooperation in cybersecurity
- Promoting cyber hygiene and awareness through information campaigns and including cybersecurity as part of academic curricula.

Input requested

- The EC Communication does not include any reference to the insurance sector's role in tackling cyber risks. The secretariat is of the opinion that there is a need to stress again, notably vis-à-vis the Commission, the important contribution of the sector. Members are invited to indicate whether they agree and if so, to suggest specific messages that can be used to achieve this (eg by making specific reference to one or several of the actions listed above).

New role of ENISA: European Cybersecurity certification framework

The EC's proposal for a regulation gives ENISA a permanent mandate as an agency and linked to this mandate, further resources and budget. Also, it introduces a European Cybersecurity certification scheme under ENISA as the new "Cybersecurity Agency".

The EC suggests that the current landscape of cybersecurity certification of ICT products and services in the EU is patchy. In the absence of an EU-wide cybersecurity certification scheme, companies in many circumstances have to be certified individually in each member state, thus leading to market fragmentation.

- The proposal does not introduce directly operational certification schemes; it creates a system – framework - for the establishment of specific certification schemes for specific ICT products/services (the "European cybersecurity certification schemes"). ENISA would thus have a central role in certification.
- The purpose of a European cybersecurity certification scheme is to attest that the ICT products and services that have been certified in accordance with such scheme comply with specified cybersecurity requirements.
    - This for instance would include their ability to protect data (whether stored, transmitted or otherwise processed) against accidental or unauthorised storage, processing, access, disclosure, destruction, accidental loss or alteration.
    - EU cybersecurity certification schemes **would not develop the technical standards themselves.** Rather, they would make use of existing standards in relation to the technical requirements and evaluation procedures that the products need to comply with.
- The proposal establishes the minimum content of such schemes. They will have to define, among others, a number of specific elements setting out the scope and object of the cybersecurity certification. This includes:
    - The identification of the categories of products and services covered
    - The detailed specification of the cybersecurity requirements (for example by reference to the relevant standards or technical specifications)
    - The specific evaluation criteria and methods
    - The level of assurance they are intended to ensure (i.e. basic, substantial or high).

- **Recourse to European cybersecurity certification should therefore remain voluntary**, unless otherwise provided in European Union legislation laying down security requirements of ICT products and services.
- In order to ensure harmonisation and avoid fragmentation, national cybersecurity certification schemes or procedures for the ICT products and services covered by a European cybersecurity certification scheme will cease to apply from the date established in the implementing act adopting the scheme.
- The monitoring, supervisory and enforcement tasks lie with the member states. Member States will have to provide for one certification supervisory authority. This authority will be tasked with supervising the compliance of conformity assessment bodies, as well as of certificates issued by conformity assessment bodies established in their territory, with the requirements of this Regulation and the relevant European cybersecurity certification schemes.

Input requested:

- Do members see any value in an EU cybersecurity certification scheme? Could it have any potential influence on insurance? For instance, could it lead to higher safety, and as a result lower premiums?
- Any other views?

Next steps

- The Commission's proposal will be discussed in the European Parliament and the Council over the coming months. The European Parliament's Industry Committee (ITRE) has the lead in these discussions, with the budgets (BUDG) and internal market (IMCO) committees issuing opinions.
    - The timeline for these discussions is not yet confirmed.